

Claims

What is claimed is:

- 1 1. In a server, a method comprising:
 - 2 registering a first party as a party relying upon a second party's certificate;
 - 3 revoking the second party's certificate after registering the first party; and
 - 4 initiating communication with the first party to indicate that the second party's
 - 5 certificate has been revoked.

- 1 2. The method of claim 1 wherein revoking the second party's certification further
- 2 comprises:
 - 3 receiving a request to revoke the second party's certificate; and
 - 4 revoking the second party's certificate in accordance with a revocation policy
 - 5 associated with the second party's certificate in response to the request.

- 1 3. The method of claim 2 wherein initiating communication with the first party further
- 2 comprises sending a revocation message to a machine that is associated with the first
- 3 party.

- 1 4. The method of claim 3 further comprising the machine associated with the first party
- 2 verifying the authenticity of the revocation message and modifying access control
- 3 information of the machine to indicate the revocation of the second party's certificate.

- 1 5. The method of claim 2 wherein accepting the request to revoke the second party's
- 2 certificate comprises accepting the request by authenticating a signature incorporated
- 3 in the request with one of a list of revoker certificates associated with the second
- 4 party's certificate.

1 6. The method of claim 2 wherein the server initiating communication with a first party
2 further comprises the server sending an email message to an email address for the
3 first party.

1 7. In a server, a method comprising:
2 registering an user as a party relying upon a digital certificate for a web site, the
3 certificate to verify messages from the web site;
4 receiving a request to revoke the digital certificate of the web site after registering
5 the user;
6 authenticating the request in accordance with a pre-defined policy;
7 revoking the digital certificate of the web site in response to the request; and
8 initiating communication with the user to indicate that the digital certificate of the
9 web site has been revoked.

1 8. The method of claim 7 wherein initiating communication with the user to indicate
2 that the digital certificate of the web site has been revoked further comprises:
3 sending a message directly to a machine associated with the user, to indicate that
4 the web site's digital certificate has been revoked.

1 9. The method of claim 8 further comprising, in the machine used by the user:
2 authenticating the message to verify that it was sent by the server; and
3 changing settings for web access to reflect the revocation of the digital certificate
4 of the web site.

1 10. The method of claim 7 wherein authenticating the request in accordance with a pre-
2 defined policy comprises authenticating a digital signature incorporated in the request

3 with a list of digital certificates previously defined as revoker certificates for the web
4 site.

1 11. A processor based server system comprising:
2 a registration database to register a first party as a relying party for a second
3 party's certificate;
4 a revocation module to revoke the second party's certificate after the first party is
5 registered; and
6 an interface with a communication network to initiate communication to indicate
7 to the first party that the second party's certificate has been revoked.

1 12. The processor based server of claim 11 further comprising:
2 a machine readable medium accessible from a processor of the server having
3 stored thereon an acceptance policy in accordance with which a revocation
4 request received via the interface may be accepted, and further having stored
5 thereon a revocation policy in accordance with which the second party's
6 certificate may be revoked.

1 13. The processor based server of claim 12, wherein the revocation module is operable to
2 send a revocation message to a machine that is associated with the first party, via the
3 interface.

1 14. A processor based server comprising:
2 a registration database to register a user as a relying party for a digital certificate
3 of a web site, the certificate to verify messages from the web site;

4 a machine readable medium accessible from a processor of the server having
5 stored thereon an acceptance policy in accordance with which a revocation
6 request received via an interface to communication network may be accepted,
7 and further having stored thereon a revocation policy in accordance with which
8 the digital certificate of the web site may be revoked in response to the revocation
9 request;
10 a revocation module to revoke the digital certificate of the web site in accordance
11 with the revocation policy; and
12 an interface with a communication network to indicate to the user that the web
13 site's certificate has been revoked.

- 1 15. The processor based server of claim 12, wherein the revocation module is operable to
2 send a revocation message to a machine operable by the user to access the web site.
- 1 16. A machine readable medium having stored thereon data which when accessed by a
2 machine cause the machine to perform the method of claim 1.
- 1 17. The machine readable medium of claim 16 having stored thereon further data which
2 when accessed by the machine cause the machine to perform the method of claim 2.
- 1 18. The machine readable medium of claim 17 having stored thereon further data which
2 when accessed by the machine cause the machine to perform the method of claim 3.
- 1 19. The machine readable medium of claim 18 having stored thereon further data which
2 when accessed by the machine cause the machine to perform the method of claim 4.

1 20. The machine readable medium of claim 17 having stored thereon further data which
2 when accessed by the machine cause the machine to perform the method of claim 5.

1 21. The machine readable medium of claim 17 having stored thereon further data which
2 when accessed by the machine cause the machine to perform the method of claim 6.

1 22. A machine readable medium having stored thereon data which when accessed by a
2 machine cause the machine to perform the method of claim 7.

1 23. The machine readable medium of claim 22 having stored thereon further data which
2 when accessed by the machine cause the machine to perform the method of claim 8.

1 24. The machine readable medium of claim 23 having stored thereon further data which
2 when accessed by the machine cause the machine to perform the method of claim 9.

1 25. The machine readable medium of claim 22 having stored thereon further data which
2 when accessed by the machine cause the machine to perform the method of claim 10.